Amendment to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended): A method for generating filters based on data entering a network device, comprising:

classifying network flows based on one or more packets received at the network device;

performing a lookup for each of the classified network flows and building a new flow cache entry if the lookup is unsuccessful;

sending each of said network flows to a corresponding flow cache and implementing policies designated for each of said network flows;

creating separate ~~an~~ aggregate network flow summaries ~~summary~~ for each of said network flows;

analyzing at least one of said aggregate network flow summaries to detect characteristics of potentially harmful network flows; and

generating a filter to prevent packets corresponding to detected potentially harmful network flows from passing through said network device.

Claim 2 (canceled).

Claim 3 (previously presented): The method of claim 1 wherein the network flow is classified based on a source device sending a packet.

Claim 4 (original): The method of claim 3 wherein the network flow is classified based on an IP address of the source device.

Claim 5 (canceled).

Claim 6 (original): The method of claim 1 wherein analyzing at least one of said network flows comprises monitoring statistics associated with said network flows.

Claim 7 (original): The method of claim 1 further comprising propagating the generated filter to an upstream network device.

Claim 8 (previously presented): The method of claim 1 wherein sending each network flow to a corresponding flow cache is performed by hardware and analyzing said network flow is performed by software.

Claim 9 (original): The method of claim 1 further comprising sending flow records corresponding to each of said network flows to a flow analyzer operable to analyze said network flows.

Claim 10 (original): The method of claim 9 wherein the flow analyzer comprises software.

Claim 11 (original): The method of claim 1 further comprising selecting a class of said network flows to analyze based on previously analyzed network flows.

Claim 12 (original): The method of claim 1 wherein said potentially harmful network flows include denial of service attacks.

Claim 13 (original): The method of claim 1 wherein said potentially harmful network flows include a high rate of incoming packets.

Claim 14 (original): The method of claim 1 wherein detecting potentially harmful network flows comprises identifying a source address associated with said harmful network flow and generating a filter comprises generating a filter to prevent packets from said identified source from passing through said network device.

Claim 15 (previously presented): A computer program product for generating filters based on analyzed network flows, comprising:

code that separates data into different network flows;

code that creates an aggregate network flow summary for one or more of said network flows;

code that selects one or more network flows for analysis;

code that analyzes said selected network flows by reviewing said aggregate network flow summaries;

code that detects potentially harmful network flows;

code that automatically generates a filter to prevent packets corresponding to said detected potentially harmful network flows from passing through the network device; and

a computer-readable storage medium for storing the codes.

Claim 16 (original): The computer program product of claim 15 wherein the computer readable medium is selected from the group consisting of CD-ROM, floppy disk, tape, flash memory, system memory, hard drive, and data signal embodied in a carrier wave.

Claim 17 (original): The computer program product of claim 15 further comprising code that propagates said filter to an upstream network device.

Claim 18 (previously presented): A system for automatically generating filters based on data entering a network device, comprising:

a netflow device operable to receive streams of packets, separate said streams, and create a summary record containing information on each of said streams;

a flow analyzer operable to analyze said summary records and identify potentially harmful network flows; and

a filter generator operable to generate a filter based on analyzed summary records to prevent packets corresponding to said identified potentially harmful network flows from passing through the network device.

Claim 19 (original): The system of claim 18 wherein the network device comprises hardware and the flow analyzer and filter generator comprise software.

Claim 20 (original): The system of claim 18 wherein the network device comprises an ACL classifier, a lookup device, and a plurality of flow buckets.

Claim 21 (original): The system of claim 18 further comprising a filter propagator operable to send information on said filters to an upstream device and request the upstream device to create a corresponding filter.

Claim 22 (canceled).

Claim 23 (previously presented): The method of claim 1 wherein information resulting from analyzing at least one of said aggregate network flow summaries is reduced in hardware so that flow records can be analyzed by software.

Claim 24 (previously presented): The method of claim 1 wherein a group of potentially harmful packets is detected and further comprising analyzing said corresponding network flow and further refining said filter.

Claim 25 (previously presented): The method of claim 1 further comprising selecting a group of network flows to be analyzed.

Claim 26 (previously presented): The method of claim 25 further comprising passing information on the selected group of network flows to a classifier.

Claim 27 (previously presented): The method of claim 1 wherein a class of packets to be analyzed is selected based on statistics associated with an aggregate filter.

Claim 28 (previously presented). A method for generating filters for network flow, comprising:

receiving data at a network device;

classifying network flows based on one or more packets received at the network device;

analyzing one or more of said network flows;

generating a filter for one or more of said network flows;

processing each of said network flows according to a corresponding policy;

selecting a class of network flows to analyze;

analyzing said selected class of network flows; and

refining said filter for said selected class of network flows.

Claim 29 (previously presented): The method of claim 28 wherein each of said filters are generated specifically for a corresponding network flow.

Claim 30 (previously presented): The method of claim 29 wherein refining said filter comprises modifying the classification of network flows.

Claim 31 (withdrawn): A system for automatically generating and refining filters based on data entering a network device, the system comprising:

an aggregate filter operable to receive streams of packets, separate said streams according to a specified criteria, and create an aggregate network flow summary for each stream of packets;

a flow analyzer operable to analyze data associated with said aggregate filter; and

a filter generator operable to refine said aggregate filter based on information received from the flow analyzer.

Claim 32 (currently amended): The system of claim ~~31~~ 18 wherein the flow analyzer is configured to identify if a rate of traffic exceeds ~~the~~ a sampling capability of the aggregate filter.

Claim 33 (currently amended): The system of claim 32 further comprising an aggregate filter operable to receive streams of packets, separate said streams according to a specified criteria, and create an aggregate network flow summary for each stream of packets and means for splitting the aggregate filter into multiple subaggregate filters if the rate of traffic exceeds the sampling capability of the aggregate filter.

Claim 34 (previously presented): The system of claim 32 further comprising a rate-limiting policer to prevent system overload.

Claim 35 (currently amended): The system of claim ~~31~~ 18 further comprising a netflow directory comprising a plurality of flow cache entries and configured to build new flow cache entries for network flows without a corresponding flow cache.

Claim 36 (previously presented): The computer program product of claim 15 further comprising code that refines said filter based on said analyzed network flow.